Jurnal Teknologi

Full paper

Traditional Security Risk Assessment Methods in Cloud Computing Environment: Usability Analysis

Sameer Hasan Albakri, Bharanidharan Shanmugam*, Ganthan Narayana Samy, Norbik Bashah Idris, Azuan Ahmed

Advanced Informatics School (AIS), Universiti Teknologi Malaysia, Malaysia

*Corresponding author: bharani.kl@utm.my

Article history

Received :10 December 2014
Received in revised form :
1 February 2015
Accepted :12 February 2015

Abstract

The term "Cloud Computing" has become very common in our daily life. Cloud computing has emerged with promises to decrease the cost of computing implementation and deliver the computing as service, where the clients pay only for what he needed and used. However, due to the new structure of the cloud computing model, several security concerns have been raised and many other security threats have been needed to be reevaluated according to the cloud structure. Besides, the traditional security risk assessment methods become unfit for cloud computing model due to its new distinguished characteristics. In this paper, we analysis the traditional information security risk assessment methods' ability to assess the security risks in cloud computing environments.

Keywords: Security risk assessment; cloud computing; security risk assessment in cloud computing

1.0 INTRODUCTION

Since cloud computing terminology introduced by Google CEO, Eric Schmidt in 2006 [1], many research efforts have been conducted. The terminology and its related technology have improved rapidly from its introductory phase. The basic idea of cloud computing is to deliver the computing resources as utility, just like the electric power; where the end-user has not to worry about how or where these resources are created or managed. It is the same concept, but with information technologies where computing (i.e. processing, storage, data, and software resources) delivering as utility; in which the providers will deliver the computing service on-demand and the consumers will pay based on usage [2]. Despite, in todays, the term cloud computing is more popular with cloud computing storage; the cloud computing model will be the most spread computing model in the next few decades. According to the National Institute of Standards and Technology (NIST), the important characteristics of cloud computing include on-demand self-service, broad network access, resources pooling, rapid elasticity, and measured service. There are three main service models; first, software as a service (SaaS), in which the consumer has capability only to use and control the application and its configuration. Second, platform as a service (PaaS) in which the consumer can control the hosting environments. Finally, infrastructure as a service (IaaS) in which the consumer has the capability to control everything except the data center infrastructure. In addition, there are four main deployment models: public clouds, private clouds, community clouds, and hybrid clouds [3].

The great features of the cloud computing model encourage the informatics system's managers to immigrate to the cloud computing environments. Kim Mays predicted that Small and Midsize Business (SMB) have or are considering adopting some sort of cloud computing technology; according to the surveys, 61 percent of SMBs are using cloud-based technologies [4]. Moreover, an IDC report says that three out of ten midsize organizations will adopt public cloud solutions [4].

Information is one of the most organizations' important assets; thus, assessing the information security risk is vital for the organizations. Information security risk assessment is important because the data confidentiality, integrity and availability could be compromised if it disclosed for unauthorized person, or modified wrongly or may be destroyed. Cloud computing raises many security risks that must be clearly addressed and assessed before moving our valuable data to the cloud computing environment. Failure to do may lead to lose the data confidentiality, integrity, and availability, which may cause a serious damage to the organization's information assets.

It is essential that every organization must have a sound risk management process within their business life cycle. The objective of the risk management is to reduce the risk to an acceptable level. The information security risk can be defined as potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organization [5]. A proper risk management process should ensure that the suitable security

controls have been used to ascertain that the organization can perform its mission [6]. There is no one can guarantee hundred percent of the security of information systems; however, the efficient and effective information security risk assessment method can provide high-level of security confidence [7].

There are many of the information security risk assessment methods, standards and regulations such as NIST SP800-30, ISO 27005 and AS/NZS 4360. They are released by governmental and private organizations such as the National Institute of Standards and Technology (NIST) and the International Organization for standardization (ISO). Despite, there is a similarity between these standards in the main steps of risk management, and there are many differences in details, phases and supporting guidelines. We can summarize the main steps of the security risk management as follows; context establishment, risk assessment, risk treatment, and risk monitoring and review. Nevertheless, most of the traditional risk assessment methodologies assume that the organization's asset is governed by the organization itself and that all security management processes are imposed by the organization. These assumptions may do not apply to cloud computing environments.

In fact, there are some main differences between cloud computing environments and conventional computing environment. These major differences make the traditional risk assessment methods are unfit for cloud computing environments. In this paper, we analyzed the ability of the traditional information security risk assessment methods' to assess the security risks in cloud computing environments. To do that, we analyzed the cloud computing security threats according to the cloud computing distinguished characteristics. Besides, we reviewed some of the existing risk assessment approaches that have been used with cloud computing.

This paper is organized as follows; the next section discusses the security threats that accompany the cloud computing model. Section three introduces some of the literature review of the current methods that used for risk assessment in cloud computing. Then, section four discusses why the current risk assessment is unfit for cloud computing, and the last section is the conclusion.

2.0 CLOUD COMPUTING SECURITY

NIST in its definition for cloud computing [3] mentioned five key features; resource pooling, broad network access, on-demand self-service, rapid elasticity, and measured service. These five key features of the cloud computing model distinguish the cloud environment from the traditional environment. Nevertheless, many security concerns accompany these characteristics or the technologies that used to guarantee provision of these characteristics. In this section, we discuss these information security threats that make the traditional risk assessment methodologies are unfit to be used in cloud computing environments.

Resource pooling: Resource pooling means that multiple clients share the resources (i.e. Processing, storage, etc.) of the same physical cloud infrastructure; they get their resource needs from the resource pool and release them when they finished. The Cloud Clients (CCs) will use the resources that offered by the Cloud Service Provider (CSP) to manage and process their own assets (i.e. Data), which means involving of different stakeholders within the process. At this point, we want to focus on these two concepts and their security problems; multi-tenancy and multi-stakeholders.

Multi-tenancy is the situation where an application runs on the CSP's server and serves the multi-client, with keeping all their data isolated [8]. However, the tenant's data will be located in the same physical memory with other tenants' data at the same time. This situation is very risky; it can cause a serious vulnerability for the confidentiality and privacy of the tenants' data. The main security concern is how the CSP can guarantee the isolation of the tenants' data. Thereby, the research efforts have different forms; some are focusing on how the re-engineering of SaaS application can extend the application capabilities to isolate the tenants' data, such as [9, 10]; while some others are focusing on how to isolate the tenants' data during its processing, rest and transition such as [11, 12] and the developing of the security controls with considering the multi-tenancy problem is also another form such as [14, 15]. The current research efforts are more about tenant oriented security than service oriented security, such as [13].

Multi-Stakeholders: In conventional information systems, there is one or more of the stakeholders, but in the cloud computing model, there are at least two stockholders (i.e. CSP and CC). This fact will affect on some security factors such as the trust between stakeholders, the compliance regulations, the decisions of the security management process, and the security tasks and responsibilities.

Asset's owner: Some security standards distinguish between 'asset ownership' and 'asset property'. The asset owner may not have the property rights to the asset, but he has the responsibility to produce, develop, maintain and use the asset [14]. In cloud computing, data as asset is maintained by the CSP but it is produced by the CC who has the property rights for the data asset. The CC is the only one who knows the value of the data and its lawfulness. Moreover, in cloud computing, we need to distinguish between two types of assets; the hardware assets and software assets. The hardware assets are owned and controlled by the CSP, but the software assets (i.e. applications and data) may be owned by the CSP or the CCs. The client's software assets (i.e. data) are under the client's property rights, but it is existed on the CSP's hardware.

Broad Network Access: the cloud computing service must be accessible by any network-based appliance such as desktop, laptop, smart-phone and tablet device. These devices can be less processing power, because the processing load will be on the CSP infrastructure. Usually, the CCs' devices use the web browsers to access to the service available on the network. In case of cloud computing, sometimes the CC's devices need to support more specialized software to deal with the virtual services. However, the cloud dependence on the network as mean of access will bring the network security concerns to the cloud computing environments.

Moreover, the concept of system boundaries will change in cloud computing environments. It is important to define the system boundaries are to ensure that all relevant assets are included during the risk assessment process. According to ISO27005, the scope and boundaries can be defined by defining the origination's constraints. In cloud computing, some constraints can be specified by the CSP such as the technical and infrastructural constraints, and others can be defined by the CCs such as legislative and regulatory constraints. In the traditional information system, the network devices and firewalls are used to define a clear boundary for the inside environment and monitor the outside access the system. However, this is not applicable for cloud computing environment since it totally depends on the network as an essential mean of access, and the main form of access is the remote access.

Besides, the cloud computing model inherits the Internet security threats; this is normal since the Internet is usually used to deliver the cloud computing services. As a result, the phishing, data loss, password weaknesses, botnets running on the client devices and username brute forcers are some examples of well-known Internet threats that will accompany the cloud computing [15].

On-demand self-service: On-demand self-service means the cloud computing service is always available for the clients. Moreover, the cloud computing service must be modifiable by the consumers with minimum interaction from the provider. The availability is one of the most important security requirements.

Some clients need to be available all the time, so they select the cloud model to guarantee unlimited resources that support their availability. However, the sharing of resources between the clients may lead to exhaust the resources which may cause a critical problem for some clients. The CSP should ensure that the clients will get enough resources whenever they need, as the unplanned downtime may cause high economic impacts. Moreover, the availability of the system may be affected by a security breach; the system must be able to continue operation even the security breach occurs [16].

Rapid elasticity: Rapid elasticity means that cloud computing provider may at least semi-automatically (i.e. near real-time) to handle the sudden increase or decrease of usage. The CSP must be able to expand or reduce allocated resources according to the consumers' requirements. This operation might be done automatically, quickly and efficiently [17]. Many problems may arise with this situation, such as data remanence and virtualization security problems.

Data Remanence: The security concern is when the tenant scales down and releases some of the resources; these resources will be relocated for another tenant. The attacker may apply for a large amount of storage and start trying to retrieve the data. The cloud computing provider must make sure that the pervious tenant data is securely erased before reallocate the resources to another tenant.

Virtualization is enabling the providers to use one single physical resource (i.e. Server, storage, and network) as multiple virtual machines. Virtualization is not the cloud computing, but it is enabled the cloud computing to be more flexible and scalable. Occasionally, cloud computing can be existed without virtualization for many reasons such as seeking more performance [18]. However, most of the cloud computing projects are built with virtualization technology. Hypervisor or virtual machine manager (VMM) is a program that manages all the virtualization functions and allows multiple operating systems to share a single hardware host. It can be installed directly on the hardware such as Microsoft Hyper-V, Oracle VM, VMware ESX, and IBM z/VM. Alternatively, it may be running on the host operating system such as Oracle VirtualBox, Parallels, Virtual PC, VMware Fusion, and VMware Server.

There are many security concerns for using virtualization in cloud computing. The potential that the hypervisor may be compromised, and this may have a bad impact on all host VMs. This risk makes the virtualization implementation one of the importance of security concern in cloud computing [19]. In addition, the implementations of virtualization must make sure that the physical media is cleared before it can be relocated for another tenant. Moreover, the network attacks that come from the other VMs on the same physical server may be hard to detect. Thus, the traffic of the VMs must be monitored. The configuration of network switches and routers must be checked and maybe reset before relocating the resource for the new tenant.

■3.0 SECURITY RISK ASSESSMENT IN CLOUD COMPUTING

The cloud computing model has certain unique characteristics and uses techniques that have raised several new risks and the need to reevaluate and redefine many well-defined past risks according to the cloud computing model [16]. Extensive research efforts were focused on defining cloud computing risks. Analyst firm Gartner published in 2008, a report on cloud computing, where it warned customers to select their cloud computing provider very carefully and to consider seven specific security issues: privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support, and long-term viability [20]. Based on previous studies, [21] thirty-two risks were identified, some new, some pre-existing. Some studies on cloud computing assessed the security risks from the clients' perspective and identified twenty-three risks [22]. ENISA published its own report on cloud computing security risks, which estimated risk levels based on the ISO/IEC 27005 standard, which were depending on risk probability and risk impact. The ENISA report lists thirty-five risks, which were organized into three categories: policy and organizational risks, technical risks, and legal risks [23].

Many researchers have proposed risk assessment methods in the cloud computing environment. Some of these studies focused on specific security problems, such as insider attacks, virtualization threats [24-27], data transmission with cloud computing [28] service-level agreement (SLA) [29, 30], anti-virus in the cloud service [31], denial of service attacks in the cloud [32] and identity management [33]. In addition, frameworks which are used to assess security risks in cloud computing environments as a whole process have also been proposed. Those proposals varied based on their study perspectives. Some studies proposed frameworks that can be used by the CCs and even suggested transferring some risks to the CSP or to a trusted third party.

Assessing the security risk from the client's perspective only, such as [21, 22] is overlooking the fact that the CSP owns and manages the infrastructure of the cloud environment. On the other hand, assessing the security risks from the service provider perspective only, such as [34-36] is underestimated the importance of involving the CCs in the risk assessment process. The CC opinion must be considered because they know how data security violations can affect them. Still, the CC cannot be involved in the whole risk management process because the process becomes very complicated as the number of CCs increases. CC participation must be at the minimum level and only to evaluate the necessary factors that affect the risk assessment results. In cloud computing, the physical infrastructure and sometimes the software used to process the data are owned by the CSP, whereas the data are owned by the CC, who alone knows the real consequences of losing data security. Thus, assessing the security risk from one side only leads to inaccurate risk evaluation. An ideal risk assessment methodology must be capable of considering the CC's business objectives without involving the client in all steps of the risk assessment process to minimize complexity.

■4.0 WEAKNESSES OF TRADITIONAL RISK ASSESSMENT METHODOLOGY

It is a fact that there is no computing model is hundred percent secure [37]; even though, many information security standards have been developed to secure the information in the traditional computing models. These security standards guaranteed an acceptable level of information security and gave an evidence that the best practice of information security has been used. NIST guidelines (SP 800-30, SP 800-39, SP 800-53), ISO 27000 family of standards, AS/NZS 4360, and AS/NZS ISO 31000:2009 are examples of these security standards.

Actually, most of these risk assessment standards assume that an organization's assets exist within that organization's data center and are fully managed by the organization itself, and that security management processes are determined by the organization itself [38, 39]. However, the characteristics of the cloud computing model invalidate this assumption in the case of a cloud computing model [16]; cloud computing has many differences that make these standards unfit for cloud computing environments. CSP will not be able to rely on the traditional risk assessment methods since the cloud computing environments are different from the traditional

computing environments; the traditional risk calculation will be inaccurate in cloud computing environments.

On the other hand, the CC will not be able to assess the security risks of CSP system; CSP will not provide extensive details of its security system to hinder hackers who may be pretending as clients. Even though, the CSP must provide CCs enough confidences that he has a sound risk-assessment process and guarantees the security of the client's assets (i.e. data).

Moreover, risk is defined as the probability of occurrence of a security breach multiplied by the consequence of occurrence of a security breach [14, 40-43]. The difficulty to apply this formula in cloud computing comes from the difficulty to calculate the risk impact and risk likelihood. The most popular way to calculate the value of risk impact is by assessing the possible loss if the security threat occurs. However, in cloud computing, CSP will not be able to assess the value of the possible loss, because he does not know the real value of the assets (i.e. Data). Which may differ from client to client, only the client himself, who know the actual value of the assets (i.e. data) and as a result the cost of its loose or breach.

Accordingly, let us assume for a moment that the CSP will ask the CC to provide their assessments of the risk impact or the cost of the consequences of losing the assets (i.e. data). Every single client will have his own assessment of his assets (i.e. data); these assessments will vary as the number of clients increased, and it will be a hard task to normalize these assessments to a specific range. Moreover, using a predefine scale, such as 1 to 5 or 1 to 10, may also result inaccurate assessments. If we do not have any equivalent monetary value of scale values, it will confuse the clients. On the other hand, it is difficult to define an equivalent monetary value for the clients' assets. Always it will be there are values out of the predefined range.

Even if we assumed there are no values out of the predefined range, the real problem is coming from the client's assessment. Sometimes it is difficult for the clients to assess the consequences of losing their data or assessing the consequences for their data breach, unless they experience that in the past. For example, if the CSP has an email system, the cloud client for this service can be a child at primary school or a manager at a big company. The email contains possibly worth nothing or maybe worth millions of dollars; it may be about a math homework or about important secrets that can cause a serious loss for the company if it is compromised. Both clients may give their email importance nine of ten on the consequence of lose scale.

Moreover, for some reasons, the probability of the risk, it is getting more difficult to be assessed in cloud computing environment; first, the users of the cloud computing systems are mobile users or external users [44]. Second, the CCs are accessing the system over the Internet, which is an open environment [45]. Third, the distinct clients will have distinct levels of users' security awareness. Fourth, there is a great potential that the risk is coming from the client himself.

Furthermore, Samy *et al*. research shows that traditional information security risk analysis methods have many weaknesses [46]. It is not able to identify various types of information security concurrency threats [47]. Besides, it is more focused on technology rather than emphasis on the people and process aspects of information systems. It has required a lot of time and has a higher cost, especially with medium to large organizations. Moreover, the centric approach in conducting risk assessment that used with the traditional method is not helping the users and field managers to improve their security awareness [46].

In brief, the traditional way to calculate the risk might have inaccurate results with cloud computing environments and also difficult to be used. Thus, we need a different methodology to assess the risk in the cloud computing environment. The suggested method must be able to consider both service provider and client and come out with accurate results. According to Kim *et al*., the security risk analysis method must guarantee provision of two advantages, effective monitoring of information security policies and appropriate information for the future prediction for information security risks [48].

5.0 CONCLUSION

In this paper, we analyzed the usability of the traditional security risk assessment methods in cloud computing environments. The characteristics of the cloud computing model make the traditional risk assessment methods are unfit for cloud computing environments. The security risk assessment method in cloud computing should be able to consider both cloud service provider and cloud client during the risk assessment process; moreover, it should be able to assess the security risk with without depending on the traditional measurements. In our future work, we will propose security risk assessment for cloud computing environment.

Acknowledgement

The authors would like to thank the Ministry of Education, Government of Malaysia and Research Management Centre, Universiti Teknologi Malaysia for supporting this work through the Fundamental Research Grant Scheme (FRGS) via vote number 4F237.

References

[1] Peiyu, L. I. U. and L. I. U. Dong. 2011. The New Risk Assessment Model for Information System in Cloud Computing Environment. *Procedia Engineering*. 15(0): 3200–3204.
[2] Buyya, R., J. Broberg, and A. G. s. nski. 2011. *Cloud Computing*. Wiley Online Library.
[3] Mell, P. and T. Grance. 2011. The NIST Definition of Cloud Computing. *NIST Special Publication*. 800: 145.
[4] Mays, K. Most Analysts Predict SMB Cloud Adoption to Continue Skyward Growth. 2013; Available from: http://www.itbusinessedge.com/blogs/smb-tech/most-analysts-predict-smb-cloud-adoption-to-continue-skyward-growth.html.
[5] British.Standard. 2009. Information Security Management-Overview and Vocabulary. British Standard: Switzerland.
[6] Peltier, T. R. 2005. *Information Security Risk Analysis*. CRC Press.
[7] Djemame, K., *et al*. 2011. A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems. In Cloud Computing 2011, The Second International Conference on Cloud Computing, GRIDs, and Virtualization. 119–126.
[8] Hurwitz, J. *et al*. 2009. Cloud Computing for Dummies. 1. For Dummies.
[9] Hong, C., W. Ning, and Z. Ming Jun. 2010. A Transparent Approach of Enabling SaaS Multi-tenancy in the Cloud. In Services (SERVICES-1), 2010 6th World Congress on.
[10] Hong, C. *et al*. 2009. An End-to-End Methodology and Toolkit for Fine Granularity SaaS-ization. in Cloud Computing, 2009. CLOUD '09. IEEE International Conference on.
[11] Chang Jie, G., *et al*. 2007. A Framework for Native Multi-Tenancy Application Development and Management. in E-Commerce Technology and the 4th IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services, 2007. CEC/EEE 2007. The 9th IEEE International Conference on.
[12] Pervez, Z., L. Sungyoung, and L. Young-Koo. 2010. Multi-Tenant, Secure, Load Disseminated SaaS Architecture. in Advanced Communication Technology (ICACT), 2010 The 12th International Conference on.
[13] Almorsy, M., J. Grundy, and A. S. Ibrahim. 2012. TOSSMA: A Tenant-Oriented SaaS Security Management Architecture. In Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on.
[14] British.Standard. 2011. Information Technology–Security Techniques–Information Security Risk Management. British Standard: Switzerland.

[15] Chen, Y., V. Paxson, and R. H. Katz. 2010. What's New About Cloud Computing Security? University of California, Berkeley Report No. UCB/EECS-2010-5 January, 2010. 20: 2010–5.
[16] Zissis, D. and D. Lekkas. 2012. Addressing Cloud Computing Security Issues. *Future Generation Computer Systems*. 28(3): 583–592.
[17] Krutz, R. L. and R. D. Vines. 2010. *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Wiley.
[18] Procopio, M. 2011. Cloud Computing Does Not Require Virtualization. 02-10-2012]; Available from: http://www.enterprisecioforum.com/en/blogs/michaelprocopio/cloud-computing-does-not-require-virtual.
[19] Speake, G. and V. J. R. Winkler. 2011. *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Elsevier.
[20] Brodkin, J., Gartner. 2008. *Seven Cloud-computing Security Risks. Infoworld*. 1–3.
[21] Saripalli, P. and B. Walters. 2010. QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference. 280–288.
[22] Tanimoto, S., *et al*. 2011. Risk Management on the Security Problem in Cloud Computing. In Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference on.
[23] ENISA. 2009. Cloud Computing: Benefits, Risks and Recommendations for Information Security. *The European Network and Information Security Agency (ENISA)*.
[24] Manavi, S., *et al*. 2012. Hierarchical Secure Virtualization Model for cloud. In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on. IEEE.
[25] Park, J. H., A. 2012. Virtualization Security Framework for Public Cloud Computing. *Computer Science and its Applications*. 203: 421–428.
[26] Luo, X., *et al*. 2011. Virtualization Security Risks and Solutions of Cloud Computing via Divide-Conquer Strategy. In Multimedia Information Networking and Security (MINES), 2011 Third International Conference on. IEEE.
[27] Lombardi, F. and R. Di Pietro. 2011. Secure Virtualization for Cloud Computing. *Journal of Network and Computer Applications*. 34(4): 1113–1122.
[28] Chu, C. H., Y. C. Ouyang, and C. B. Jang. 2012. Secure Data Transmission with Cloud Computing in Heterogeneous Wireless Networks. *Security and Communication Networks*. 5(12): 1325–1336.
[29] Morin, J., J. Aubert, and B. Gateau. 2012. Towards Cloud Computing SLA Risk Management: Issues and Challenges. in System Science (HICSS), 2012 45th Hawaii International Conference on. IEEE.
[30] Hammadi, A. M. and O. Hussain. 2012. A Framework for SLA Assurance in Cloud Computing. in Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on. IEEE.
[31] Yan, W. and N. Ansari. 2011. Anti-virus in-the-cloud Service: Are We Ready for the Security Evolution? *Security and Communication Networks*. 5(6): 572–582.
[32] Khorshed, M.T., A. Ali, and S.A. Wasimi. 2012.Classifying Different Denial-of-Service Attacks in Cloud Computing Using Rule-based Learning. *Security and Communication Networks*.
[33] Wang, B., *et al*. 2009. Open Identity Management Framework for SaaS Ecosystem. In e-Business Engineering, 2009. ICEBE '09. IEEE International Conference on.
[34] Xuan, Z., *et al*. 2010. Information Security Risk Management Framework for the Cloud Computing Environments. In Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on.
[35] Fito, J. O. and J. Guitart. 2012. Business-driven Management of Infrastructure-level Risks in Cloud Providers. Future Generation Computer Systems.
[36] Fito, J.O., M. Macias, and J. Guitart. 2010. Toward Business-driven Risk Management for Cloud computing. In Network and Service Management (CNSM), 2010 International Conference on.
[37] Sharma, S. 2013. Embedded Systems–A Security Paradigm for Pervasive Computing. In Communication Systems and Network Technologies (CSNT), 2013 International Conference on.
[38] Almorsy, M., J. Grundy, and A.S. Ibrahim. 2011. Collaboration-based Cloud Computing Security Management Framework. In Cloud Computing (CLOUD), 2011 IEEE International Conference on.
[39] Zhao, G. 2012. Holistic Framework of Security Management for Cloud Service Providers. In Industrial Informatics (INDIN), 2012 10th IEEE International Conference on. IEEE.
[40] Karabacak, B. and I. Sogukpinar. 2005. ISRAM: Information Security Risk Analysis Method. Computers & Security. 24(2): 147–159.
[41] Pirzadeh, L. and E. Jonsson. 2011. *A Cause and Effect Approach Towards Risk Analysis*.
[42] Blakley, B., E. McDermott, and D. Geer. 2001. Information Security Is Information Risk Management. In Proceedings of the 2001 Workshop on New Security Paradigms. ACM.
[43] Schechter, S. E. 2005. Toward Econometric Models of the Security Risk From Remote Attacks. *Security & Privacy, IEEE*. 3(1): 40–44.
[44] Xie, Q., *et al*. 2013. Secure Mobile User Authentication and Key Agreement Protocol with Privacy Protection in Global Mobility Networks. in Biometrics and Security Technologies (ISBAST), 2013 International Symposium on. IEEE.
[45] Miyazaki, A. D. and A. Fernandez. 2001. Consumer Perceptions of Privacy and Security Risks for Online Shopping. *Journal of Consumer Affairs*. 35(1): 27–44.
[46] Samy, G. N., R. Ahmad, and Z. Ismail, Adopting and Adapting Medical Approach in Risk Management Process for Analysing Information Security Risk, in Risk Management for the Future–Theory and Cases, J. Emblemsvåg, Editor. InTech.
[47] Badr, Y. and J. Stephan. 2007. Security and Risk Management in Supply Chains. *Journal of Information Assurance and Security*. 2(4): 288–296.
[48] Kim, Y.-G., *et al*. 2007. Modeling and Simulation for Security Risk Propagation in Critical Information Systems. In Computational Intelligence and Security. Springer. 858–868.